Karlsruher Institut für Technologie

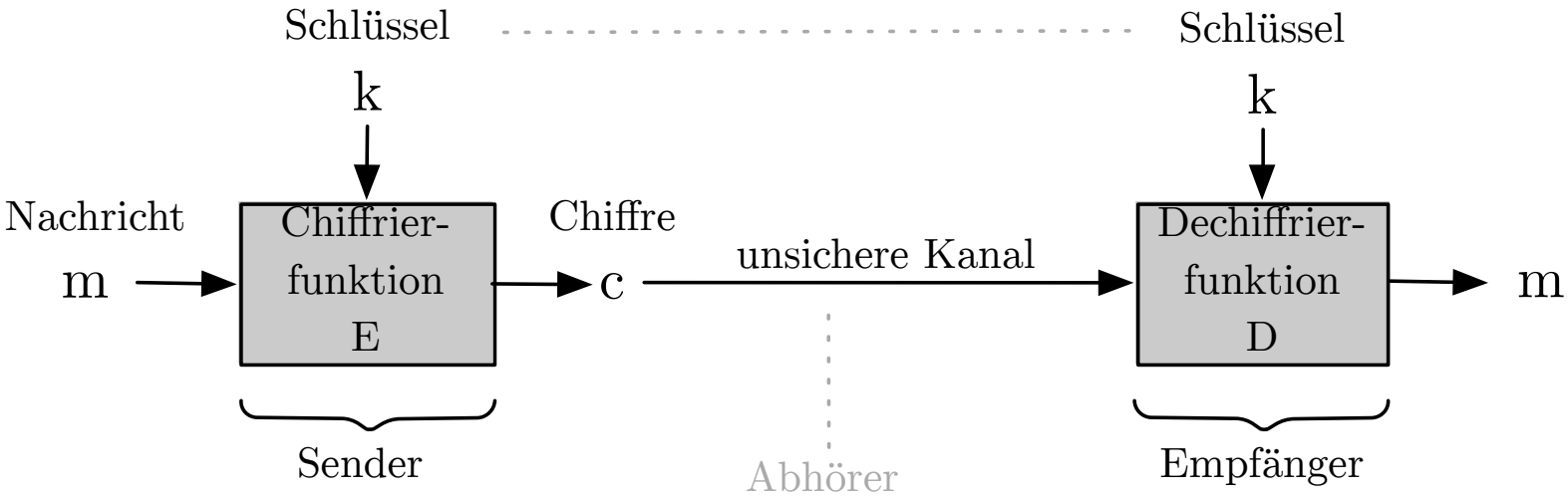
Theoretische Grundlagen der Informatik

Informationstheorie
Vorlesung vom 9. Februar 2016

INSTITUT FÜR THEORETISCHE INFORMATIK

Kryptographie

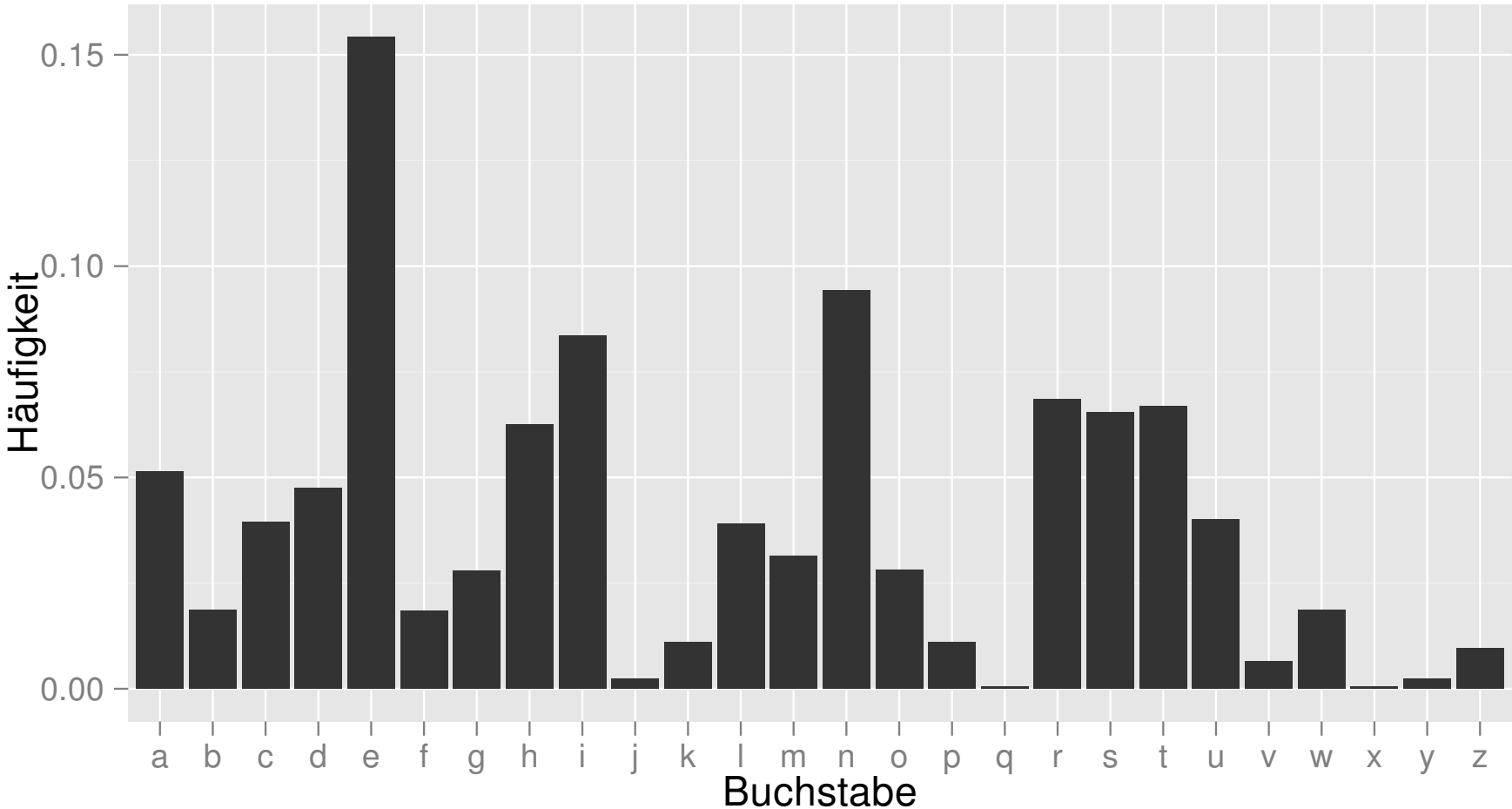
Modell eines symmetrischer Verschlüsselungsverfahren



- Nachricht m aus Nachrichtenmenge M, Schlüssel k aus Schlüsselmenge K
- Chiffre c aus Chiffremenge C
- Chiffrier-und Dechiffrierfunktionen $E : M \times K \to C$ und $D : C \times K \to M$
- Es gilt: $D(E(m, k), k) = m$

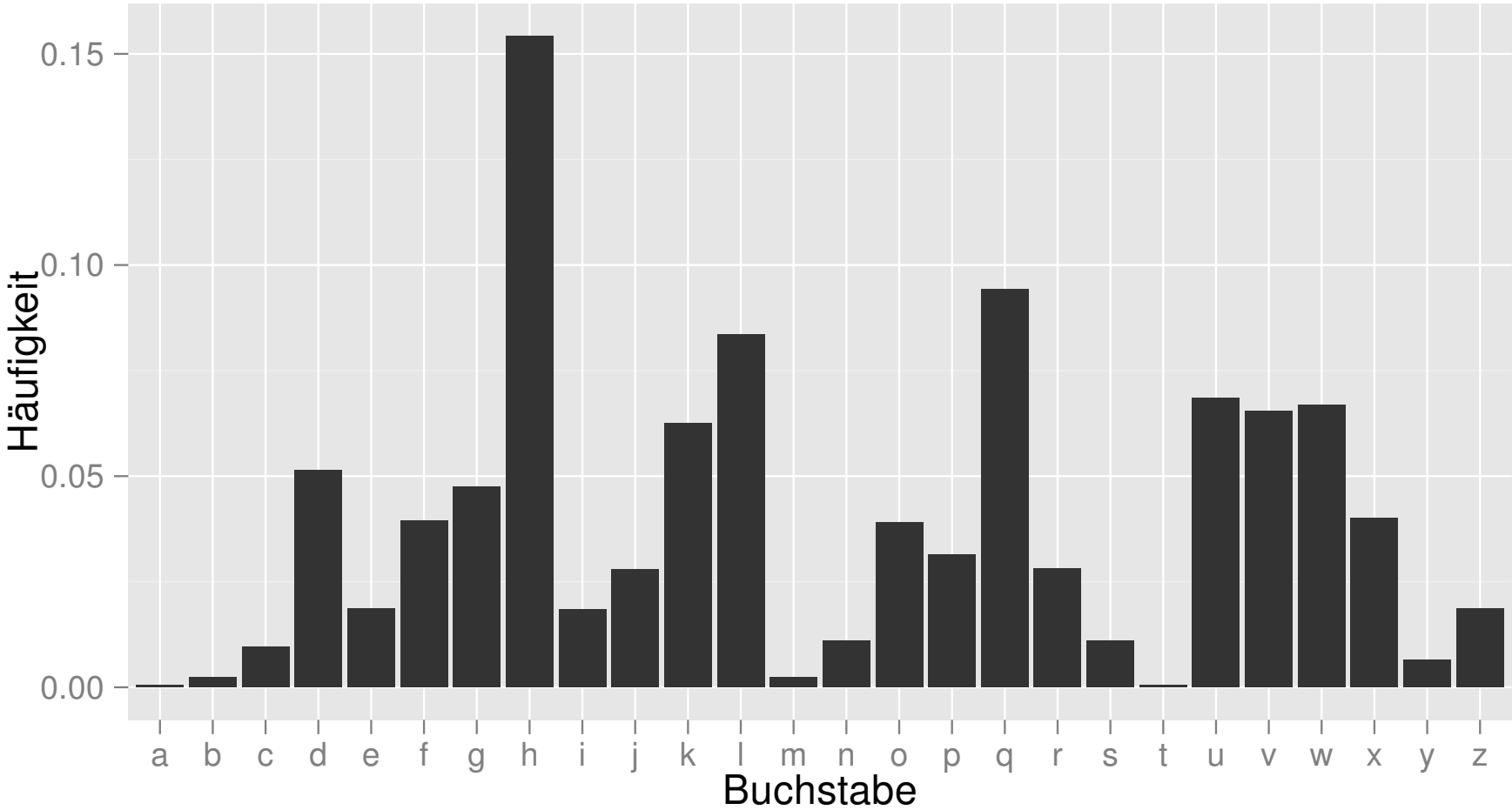
Monoalphabetische Verschiebechiffre

Nachrichtentextverteilung



Monoalphabetische Verschiebechiffre

Chiffretextverteilung ($c = E(m,k) = m + k \mod 26$, $k = 3$)



Kryptographie

Angriffsszenario auf die Kommunikation von Sender A zu Empfänger B

- Angreifer E belauscht Kommunikation zwischen A und B
- E hat beliebig große Rechner-und Speicherrresourcen

Ein Verschlüsselungsverfahren heißt perfekt sicher, wenn die *a priori Wahrscheinlichkeit* des Klartextes gleich der *a posteriori Wahrscheinlichkeit* ist.

Kryptographie

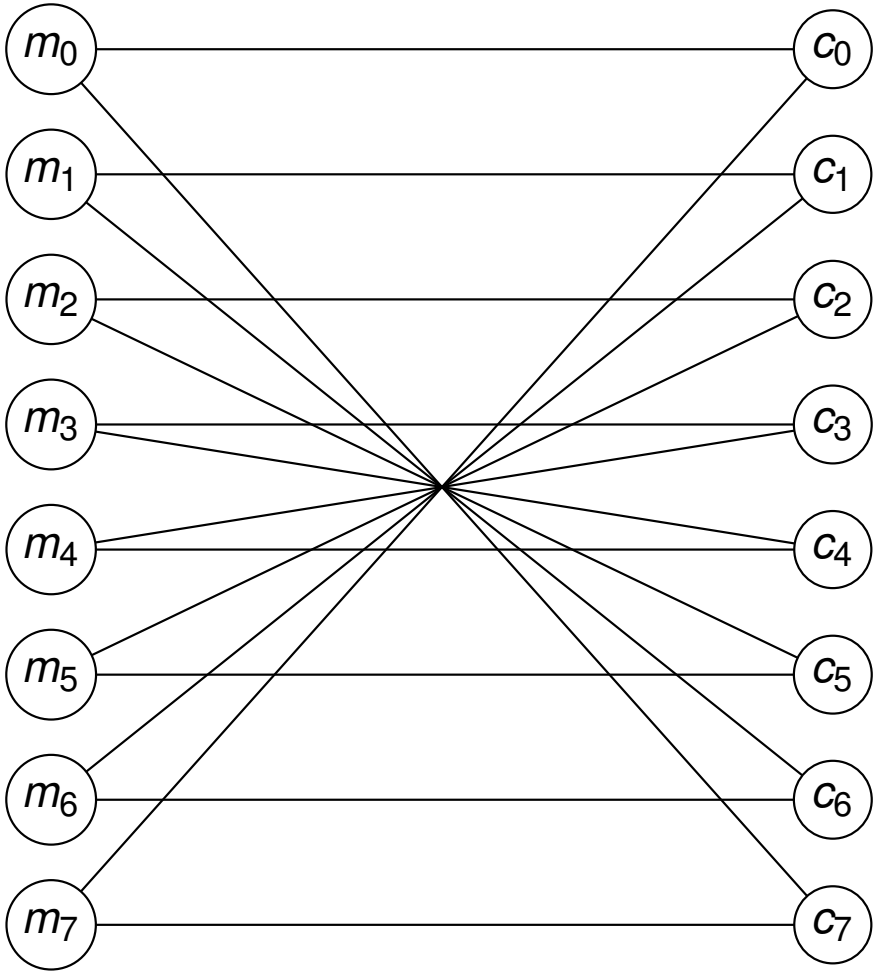
Definition
Ein Verschlüsselungsverfahren heißt *perfekt sicher* falls für alle Nachrichten $m \in M$ und Chiffren $c \in C$ gilt, dass sie stochastisch unabhängig sind, also die Gleichung $p(m) = p(m \mid c)$ gilt.

- Es gilt mit Bayes

$$p(m \mid c) = \frac{p(c, m)}{p(c)} = \frac{p(c \mid m) \cdot p(m)}{p(c)}$$

- Somit ist also auch $p(c \mid m) = p(c)$.

Kryptographie

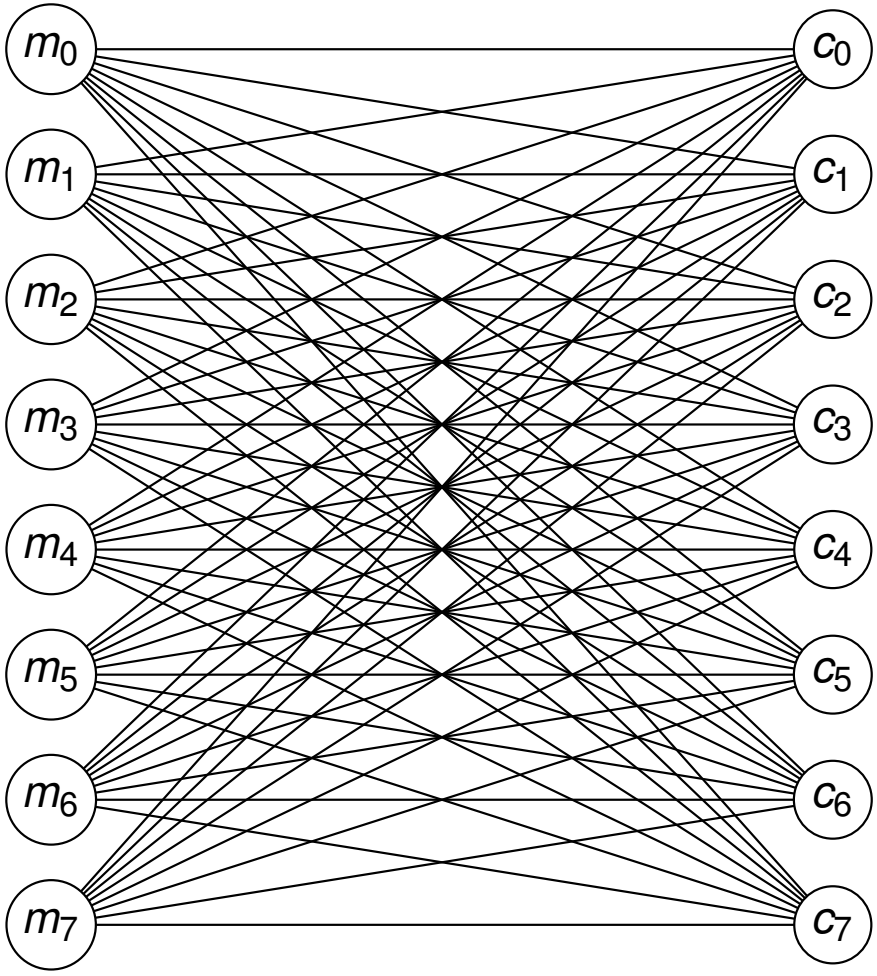


Graph:

- Knoten links: Nachrichtenmenge
- Knoten rechts: Chiffremenge
- Kante zwischen m_i und c_j: Schlüssel k mit $E(m_i, k) = c_j$

Monoalphabetische Verschiebechiffre (Cäsar-Chiffre), hier für ein binäres Alphabet und Nachrichtenlänge 3.

Kryptographie



Graph:

- Knoten links: Nachrichtenmenge
- Knoten rechts: Chiffremenge
- Kante zwischen m_i und c_j: Schlüssel k mit $E(m_i, k) = c_j$

Vernam-Chiffre:

- Vollständiger bipartiter Graph
- $|M| = |C| = |K|$
- Jeder Schlüssel gleich wahrscheinlich

Perfekt Sicherheit
Ein Kryptosystem (M, K, C) ist *perfekt sicher*, gdw. $H(M) = H(M|C)$. Die Entropie – also die Unsicherheit über die Nachricht – wird nicht verringert, wenn die Chiffre bekannt ist.

Beweis „$\Rightarrow$”: Mit perfekt sicher gilt: $p(m,c) = p(m) \cdot p(c)$.

$$
\begin{aligned}
H(M \mid C) &= \sum_M \sum_C p(m,c) \log \frac{1}{p(m \mid c)} \\
&= \sum_M \sum_C p(m) \cdot p(c) \log \frac{1}{p(m)} \\
&= \sum_M p(m) \log \frac{1}{p(m)} \underbrace{\sum_C p(c)}_{=1} \\
&= H(M)
\end{aligned}
$$

Perfekt Sicherheit
Ein Kryptosystem (M, K, C) ist *perfekt sicher*, gdw. $H(M) = H(M|C)$. Die Entropie – also die Unsicherheit über die Nachricht – wird nicht verringert, wenn die Chiffre bekannt ist.

Beweis „$\Leftarrow$”: Mit $H(M, C) = H(M)$ ist $I(M; C) = H(M) - H(M \mid C) = 0$

$$\begin{aligned}
\Rightarrow 0 &= \sum_M \sum_C p(m,c) \log \frac{p(m|c)}{p(m)} \\
\Rightarrow 0 &= \sum_M \sum_C \underbrace{p(m,c)}_{>0} \underbrace{\log \frac{p(m,c)}{p(m) \cdot p(c)}}_{\geq 0;\ \text{muss 0 ergeben}} \\
\Rightarrow p(m,c) &= p(m) \cdot p(c) \\
\Rightarrow p(m \mid c) &= p(m)
\end{aligned}$$